Aula 07

MAIS SOBRE O GRUPO SIMÉTRICO

META

Conhecer um pouco mais de perto as propriedades do grupo das permutações de nível n.

OBJETIVOS

Reconhecer elementos de S_n

Reconhecer os subgrupos A_n e D_n de S_n

Aplicar propriedades decorrentes do teorema da representação no estado de grupos finitos.

PRÉ-REQUISITOS

As aulas 4,5 e 6.

INTRODUÇÃO

Nesta aula, caro aluno, estudaremos um pouco mais os grupos de permutação S_n, onde apresentaremos os subgrupos das permutações pares (A_n) e das simetrias de um polígono conhecido também como o subgrupo diedral (D_n). Mostraremos também nesta aula que todo grupo finito pode ser visto como um grupo de permutações, que é o conteúdo dos teoremas da correspondência e de Cayley.

SINAL DE UMA PERMUTAÇÃO E O GRUPO ALTERNADO A_n.

Definição 1. Seja $\tau \in S_n$. Dizemos que τ é uma transposição se existem $i, j \in \{1,2,\dots,n\}$, com $i \neq j$ tais que $\tau(i) = j$ e $\tau(k) = k \ \ \forall k \in \{1,2,\dots,n\} - \{i,j\}$.

Por simplicidade de notação, costumamos escrever $\tau = (ij)$.

Exemplo 1. Em S_5 $\quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$ é uma transposição que transforma 2 em 4, 4 em 2 e fixa os demais.

Indicamos: $\tau = (24)$.

Notemos que toda transformação é igual à sua inversa. $\tau^2 = e$ ou $\tau = \tau^{-1}$.

Proposição 1. Toda permutação de S_n para $n \geq 2$, pode ser escrita como um produto de transposições..

Demonstração: Vamos usar indução sobre n. Se $n = 2$, $S_2 = \{e = (12)(21), (12)\}$, ok! Suponhamos que $n > 1, \sigma \in S_n$, $k = \sigma(n)$ e $\tau = (kn)$. Então $\tau\sigma(n) = \tau(k) = n$, ou seja, $\tau\sigma$ fixa n. Logo, podemos olhar para $\tau\sigma$ como uma permutação de S_{n-1} e, por hipótese de indução existem transposições de S_n que fixam n tais que $\tau\sigma = \tau_1\tau_2 \dots \tau_s$. Portanto, $\sigma = \tau^{-1}\tau_1.\tau_2 \dots \tau_s$.

Exemplo 2. Em S_4, seja $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$.

Notemos que:

$\sigma = (12)(23)(24)$ e também $\sigma = (13)(14)(12)(24)(13)(24)(13)$

Este exemplo mostra que não é única a forma de expressar uma permutação como um produto de transposições, inclusive o número de transposições.

Na realidade pode-se provar que duas fatorações de uma permutação como produtos de transposições têm em comum a paridade do número de fatores. No exemplo acima as fatorações têm 3 e 7 fatores (ambos ímpares).

Definição 2. Seja $\sigma \in S_n \ (n \geq 2)$. Dizemos que σ é uma permutação par se é par o número de fatores de uma (e, portanto de todas) fatoração como produto de transposições. Quando σ não é par, dizemos que σ é impar.

Segue da definição acima que o produto de duas permutações de mesmo paridade é par e que o produto de duas permutações com paridades distintas é impar. É fácil ver também que σ e σ^{-1} têm a mesma paridade $(\sigma = \tau_1 \dots \tau_n \Longrightarrow \sigma^{-1}. \tau_n \dots \tau_1)$ e que a identidade e é par $(\tau\ transposição \Longrightarrow e = \tau . \tau)$.

Podemos, dos comentários acima, concluir que é válida a

Proposição 2. O conjunto A_n de todas as permutações pares de nível n é um subgrupo de S_n. (Este subgrupo é também conhecido como o grupo alternado de $nível\ n$).

Seja $I = \{-1,1\}$ o grupo multiplicativo de ordem 2, e seja

$$\begin{aligned} \varepsilon : S_n &\longrightarrow I \\ \sigma &\rightsquigarrow \varepsilon(\sigma) \end{aligned}$$

$\varepsilon(\sigma) = 1$ se σ é par e $\varepsilon(\sigma) = -1$ se σ é impar. Então, ε é um homomorfismo sobrejetivo com núcleo A_n.

Do 1º teorema dos homomorfismos segue que $A_n \trianglelefteq S_n$ e $\frac{S_n}{A_n} \cong I$.

Portanto, $\left|\frac{S_n}{A_n}\right| = 2$ e, do teorema de lagrange segue que $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

Um artifício para testar a paridade de um $\sigma \in S_n$ é o seguinte: sejam $X_1, X_2, \dots, X_n$ n variáveis e seja $P = (X_1 - X_2)(X_1 - X_3) \dots (X_{n-1} - X_n) = \Pi_{i<j}(X_i - X_j$ polinômio nestas variáveis. Para cada $\sigma \in S_n$, definamos

$P^\sigma = \left(X_{\sigma(1)} - X_{\sigma(2)}\right)\left(X_{\sigma(1)} - X_{\sigma(3)}\right) \dots (X_{\sigma(n-1)} - X_{\sigma(n)})$. Logo, $P^\sigma \in \{P, -P\}$.

Se $P^\sigma = P$ então σ é par e se $P^\sigma = -P$, σ é impar.

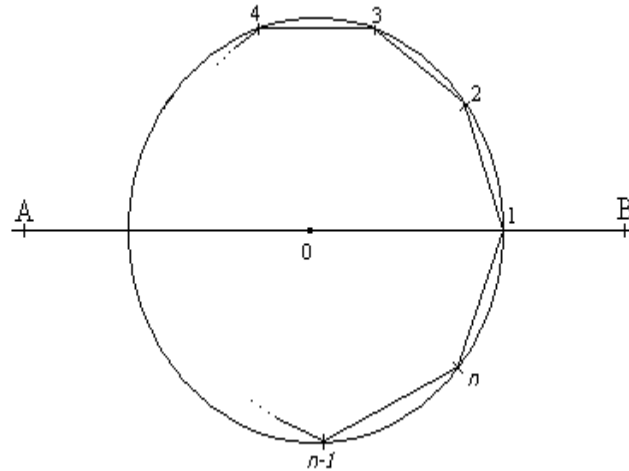
Exemplo 3. Seja $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3$.

Então $P^\sigma = \left(X_{\sigma(1)} - X_{\sigma(2)}\right)\left(X_{\sigma(1)} - X_{\sigma(3)}\right) \dots \left(X_{\sigma(2)} - X_{\sigma(3)}\right) = (X_3 - X_1)(X_3 - X_2)(X_1 - X_2) = (X_1 - X_2)(-(X_2 - X_3))\left(-(X_1 - X_3)\right) = P$

Logo, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ é par.

Exemplo 4. Verificando diretamente, $A_n = \left\{e, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\right\}$

O SUBGRUPO DIEDRAL D_n DE S_n

Seja $I = \{1,2,\dots,n\}, n \geq 3$. Vamos identificar os elementos de I_n como os vértices de um polígono regular de n lados de centro O, como na figura:

Olhando para S_n como o grupo de todas as permutações do conjunto de vértices I_n, vamos agora estabelecer um subgrupo de S_n contendo exatamente $2n$ elementos.

Indiquemos por θ a permutação de S_n obtida quando giramos o polígono de $\frac{360°}{n}$ no sentido trigonométrico, ou seja:

$$\theta = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix} \text{ e}$$

indiquemos por r a permutação de S_n obtida quando fazemos a reflexão do polígono em torno do eixo AB, ou seja:

$$r = \begin{pmatrix} 1 & 2 & \dots & \frac{n+2}{2} & \dots & n-1 & n \\ 1 & n & \dots & \frac{n+2}{2} & \dots & 3 & 2 \end{pmatrix} \text{ se } n \text{ é par ou } r = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix} \text{ se } n \text{ é impar.}$$

Definição 3. Chamamos subgrupo diedral D_n de S_n ao conjunto de todas as permutação σ que podem ser escritas como uma expressão do tipo

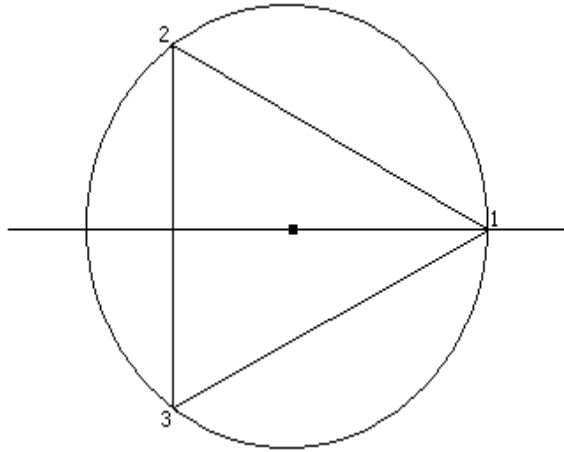
$\sigma = \theta^{m_1} r^{n_1} \theta^{m_2} r^{n_2} \dots \theta^{m_k} r^{n_k}$ onde $m_{1,} n_1, \dots, m_{k,} n_k \in \mathbb{Z}$ e $k \in \{1,2,\dots\}$.

Indicamos $D_n = < r, \theta >$

Através de uma observação cuidadosa dos efeitos de composições evolvendo r e θ, na figura, podemos concluir que:

$\theta^n = e, r^2 = e, r.\theta^i = \theta^{-i}.r$ e $\theta^{-j}.r = r.\theta^{-j}, \ \forall i,j \in \mathbb{Z}_+$.

Usando estas leis, podemos concluir ainda que $D_n =< r, \theta >= \{e, r, \theta, \theta^2, \dots, \theta^{n-1}, r\theta, r\theta^2, \dots, r\theta^{n-1}\}$ onde dados $\sigma, \tau \in D_n$, $\sigma\tau^{-1} \in D_n$ sempre. Ou seja D_n é um subgrupo de S_n contendo exatamente $2n$ elementos. D_n é o subgrupo menos amplo de S_n que contém θ e r.

Exemplo 5. Para $n = 3, D_3 = S_3$, pois

$$\theta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \qquad r = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$\theta^3 = e,\ r^2 = e.$

$\Longrightarrow D_3 =< r, \theta \geq= \{e, r, \theta, \theta^2, r\theta, r\theta^2\}$ e como $|D_n| = 6 = |S_3|$,segue que $D_3 = S_3$.

OS TEOREMAS DA REPRESENTAÇÃO E DE CAYLEY

Proposição 3.(Teorema da representação).Sejam G um grupo e $H \leq G$ tal que $[G : H] = n$. Então existe um subgrupo normal N de G tal que $N \trianglelefteq H$ e, a menos de isomorfismo, $\frac{G}{N} \leq S_n$. Além disto, se $L \trianglelefteq G$ e $L \leq H$ então $L \leq N$.

Demonstração: sejam $G/_H = \{Ha_1, Ha_2, \dots, Ha_n\}$ o conjunto quociente de G módulo H e P o grupo simétrico (das permutações) de $G/_H$. Consideremos agora a aplicação $\psi : G \longrightarrow P$ onde, para cada $a \in G$, $\psi(a) : \frac{G}{H} \longrightarrow \frac{G}{H}$ é dada por $\psi(a)(Ha_i) = Ha_i a^{-1}$.

Notemos que $\psi(a)(Ha_i) = \psi(a)(Ha_j) \Leftrightarrow Ha_i a^{-1} = Ha_j a^{-1} \Leftrightarrow$

$\Leftrightarrow a_i a^{-1}.(a_i a^{-1})^{-1} \in H \Leftrightarrow a_i a^{-1} a a^{-1} \in H \Leftrightarrow a_i \equiv a_j (mod\ H) \Leftrightarrow Ha_i = Ha_j$, ou seja, para cada a, $\psi(a)$ é injetiva de $\frac{G}{H}$ em $\frac{G}{H}$ que é finito, logo, $\psi(a) \in P$ e conseqüentemente ψ esta bem definida.

Dados $a, b \in G, \psi(ab) : \frac{G}{H} \longrightarrow \frac{G}{H}$ é tal que $\psi(ab)Ha_i = Ha_i(ab)^{-1} = Ha_ib^{-1}a^{-1} = \psi(a)(Ha_ib^{-1}) = \psi(a)(\psi(b)Ha_i) = \psi(a).\psi(b)(Ha_i)$ para cada $Ha_i \in \frac{G}{H}$. Logo $\psi(ab) = \psi(a).\psi(b) \quad \forall a, b \in G$ ou seja ψ é um homomorfismo de grupos.

Por outro lado, notemos que $a \in ker\,\psi \Leftrightarrow \psi(a)Ha_i = Ha_i, \ \forall\, Ha_i \in \frac{G}{H} \Leftrightarrow Ha_ia^{-1} = Ha_i \ \ \forall Ha_i \in \frac{G}{H} \Leftrightarrow Ha_i = Ha_ia \ \ \forall\, Ha_i \in \frac{G}{H} \Leftrightarrow a_1aa_i^{-1} \in H \ \forall\, Ha_i \in \frac{G}{H} \Leftrightarrow a \in a_i^{-1}Ha_i \ \ \forall a_i \in \{a_1, \dots, a_n\}$.

Lembrando que $G = \bigcup_{i=1}^{n} Ha_i$, podemos escrever: $a \in \bigcap_{b \in G} b^{-1}Hb = \ker\psi \trianglelefteq H$

Tomando $N = \bigcap_{b \in G} b^{-1}Hb$, temos do 1º teorema do homomorfismo que $\frac{G}{N} \cong Im\,\psi \leq P \cong S_n$.

Finalmente, se $L \trianglelefteq G$ e $L \leq H$ então, $\forall b \in G,\ b^{-1}Lb = L \leq b^{-1}Hb \Longrightarrow L \leq \bigcap_{b \in G} b^{-1}Hb = N$.

Corolário (Teorema de Cayley). Se G é um grupo finito de ordem n então G é isomorfo a algum subgrupo de S_n.

Demonstração: Sendo $|G| = n$, tomando no teorema da correspondência $H = \{e\} \Longrightarrow N = H$, segue que $[G : H] = n$, donde temos $G \cong \frac{G}{N}$ e portanto, G é isomorfo a um subgrupo de S_n.

Exemplo 6. Quando G é finito é $H \leq G$ é tal que $[G : H] = p$ onde p é o menor primo positivo divisor da ordem G, temos $H \trianglelefteq G$. Com efeito, do teorema da correspondência, existe $N \trianglelefteq G$, $N \leq H$ tal que $[G{:}\,N] | p!$. Sendo p o menor divisor primo de $|G|$, do teorema de Lagrange, p é o menor divisor primo positivo de $[G : N]$. Segue então que $[G : N] = p$ e conseqüentemente $H = N$.

Em particular, se $|G|$ é par e $H \leq G$ tal que $|H| = \frac{G}{2}$, então $H \trianglelefteq G$. Ainda, como já sabíamos, para $n \geq 2$ $A_n \trianglelefteq S_n$.

ATIVIDADES

1. Quantas transposições tem S_n?

2. Qual a paridade da permutação $\sigma = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 2\,3\,4\,1\,6\,7\,5 \end{pmatrix}$.

3. Resolva em D_4, a equação $x^2 = e$.

4. Calcule $Z(D_4)$ e $Z(A_4)$.

5. Se G é um grupo tal que $|G| = p^n$, onde $p \in \mathbb{Z}_+$ é um primo, $n \in \mathbb{Z}_+^*$, e $H \leq G$ onde $|H| = p^{n-1}$, prove que $H \trianglelefteq G$.

6. Seja G um grupo e suponha que G é infinito e simples. Se H é um subgrupo próprio de G $(H \neq G)$, prove que $[G : H]$ é infinito.

COMENTÁRIO DAS ATIVIDADES

Na primeira atividade, você deve ter usado algum conhecimento adquirido no ensino médio quando estudou análise combinatória!

Na segunda atividade, como $|D_4| = 8$, você deve ter resolvido facilmente, substituindo diretamente na equação $x^2 = e$, todos os elementos de D_4.

Na quarta, você deve também ter escrito os grupos explicitamente e procurado diretamente os seus centros, lembrando sempre do teorema de Lagrange.

A quinta atividade, se você conseguiu desenvolvê-la, usou o fato de que $[G : H] = p$ que é o menor fator primo da ordem de G

Na sexta, se, por absurdo, $[G : H] = n$ fosse finito, do teorema da correspondência existiria um subgrupo normal N de G tal que $N \subset H$ onde $\frac{G}{N}$ seria um subgrupo de S_n. Sendo G simples, N seria necessariamente {e} mas, isto implicaria, $G \approx \frac{G}{\{e\}}$ que é finito.

Caro aluno, reler o texto é sempre necessário e procure os tutores sempre que necessite.

REFERÊNCIAS

GONÇALVES, Adilson. Introdução à álgebra. 5. ed. Rio de Janeiro: IMPA, 2007. 194 p. (Projeto Euclides) ISBN.

HUNGERFORD, Thomas W. Abstract algebra: an introduction. 2nd. ed. Austrália: Thomson Learning, ©1997.

GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de algebra. 3. ed. Rio de Janeiro: IMPA, 2005. 326 p. (Série: Projeto Euclides).